NetPurifier

stop pornography now!

Version 3

September 1, 2003

The products described in this User's Guide are licensed products of NetPurifier, Inc. This User's Guide contains proprietary information protected by copyright, and this User's Guide and all accompanying software and documentation are copyrighted.

NetPurifier, Inc. , hereafter referred to as NetPurifier, does not warrant that the product will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

NetPurifier has made every effort to ensure that this manual is accurate. However, information in this User's Guide is subject to change without notice and does not represent a commitment on the part of NetPurifier. NetPurifier makes no commitment to update or keep current the information in this User's Guide, and reserves the right to make changes to this User's Guide and/or product without notice. NetPurifier assumes no responsibility for any inaccuracies and omissions that may be contained in this User's Guide. If you find information in this User's Guide that is incorrect, misleading, or incomplete, we would appreciate your comments.

No part of this User's Guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of NetPurifier.

The NetPurifier logo is a trademark of NetPurifier, Inc
All other trademarks or registered trademarks listed belong to their respective owners.

Copyright 2003 NetPurifier, Inc.
All rights reserved.

Table of Contents

Table of Contents i

Introduction and Getting Started 1-1

Features 1-1

How NetPurifier Works 1-2
Overview 1-2
Filtering System 1-2
Sensitivity Levels 1-3

Using This User's Guide 1-4
Navigating Through This Online User's Guide 1-4
Conventions in This User's Guide 1-5

Getting Started 1-6

Installing NetPurifier 2-1

Installation 2-1
Location 2-1
AC Power 2-1
Network Connection 2-1
Power On and Indicator Lights 2-2

Connecting a browser to NetPurifier 2-2
Windows 2000/XP 2-3
MAC OS10 2-3

Making a connection 2-4

Configuring NetPurifier 3-1

Security Configuration 3-1
Changing the default password 3-2

DNS/Gateway Configuration 3-4
Network Interfaces (IP Address Configuration) 3-5
Routing and Gateways 3-7

DNS 3-8
Completing the DNS/Gateway Configuration 3-8

DHCP Configuration 3-9
Using an existing DHCP Server 3-9
Using the NetPurifier DHCP Server 3-9

Port Blocker 3-12
Changing Port Blocker Configuration 3-13
Enabling Common Ports 3-13
Adding User Defined Ports 3-14
Enabling All Ports 3-14
Router Compatibility Mode 3-14

Changing levels, lists and messages 3-15
Changing Levels 3-15
Filter Matrix 3-16
Adding to the Exception Site list 3-20
Adding to the Exception IP list 3-21
Changing the Access Denied page message 3-22
Add to Banned Site List 3-23

NetPurifier Operation 4-1

Network Flow 4-2

How NetPurifier filters 4-2
Blacklist 4-3
Smart Filter Technology 4-4

Troubleshooting A-1

Contact Information B-1

Location B-1

Website B-1

Sales B-1

Technical Support B-2

Specifications C-1

Chapter 1

Introduction and Getting Started

NetPurifier™ stops the pornography, the on-line gambling, the hate sites at the Internet gateway, before the offensive material reaches children. You don't have to worry about kids surfing the Net. With NetPurifier, if they accidentally misspell a word or use a search word that takes them to the "dark side," they will see a friendly message telling them the site has inappropriate content.

Features

NetPurifier offers the following features:

- Stops access to pornography, hate and gambling sites.
- Blocks downloading of harmful and illegal files including mp3 music files.
- Filters networks as large as 230 computers.
- Three types of filtering with Smart Filter Technology.
- Four sensitivity levels configured for different age groups.
- 500,000+ site Blacklist updated daily or weekly.
- Built in DHCP server.
- Built in Caching Proxy.
- Does not require reconfiguration of client computers.
- Easy to install, no required maintenance.
- Unlimited licensing is standard.

How NetPurifier Works

Overview

NetPurifier is a hardware-and-software, set-it-and-forget-it device that plugs into your network and redirects all Internet traffic to itself. Only the NetPurifier communicates directly with the Internet. Internet information for all other computers (e.g., Windows, Apple, Linux) must first go through the filter system built into the NetPurifier.

Filtering System

A three-tier filter system ensures that inappropriate content does not reach the user.

First, NetPurifier compares the site with its blacklist to determine if the address has already been deemed inappropriate.

The product then looks at the site rating, searching for the industry-standard rating tags.

Finally, NetPurifier scans every word on the Internet page looking for words that indicate inappropriate content. The context of these words is then analyzed to determine if the page should be blocked. This greatly reduces the number of false positives while blocking those pages that are offensive. This feature accounts for NetPurifier's remarkable accuracy.

If the content passes through all three filters, NetPurifier allows the page to be loaded on the user's computer. If any of the filters fail, an "Access Denied" page is sent to the user's computer. All this is done in a fraction of a second, with no delay seen by the user.

Sensitivity Levels

Level 1

This level is suggested only for the youngest children or where the strictest policy is enforced.

- Incorporates very strict filtering and minimal downloading capabilities.
- Porn, hate, hacking and gambling are not allowed.
- Web based email is not allowed at common sites such as Hotmail and Yahoo.
- Downloading of files including exe, mp3, dll, avi, visual basic extensions and many more are not allowed.
- Many automatic program updates will not work with this setting.

Level 2

This level is suggested for Elementary Schools

- Porn, hate, hacking and gambling are not allowed.
- Web based email is not allowed at common sites such as Hotmail and Yahoo.
- Downloading of files, excluding mp3 and exe, is allowed.

Level 3

This level is suggested for Middle or Junior High Schools

- Porn, hate, hacking and gambling are not allowed.
- Web based email allowed.
- Downloading of files, excluding mp3, is allowed.

Level 4

This level is suggested for public access points such as kiosks and library terminals, High School and colleges and filtered adult use.

- Porn is not allowed.
- Web based email allowed.
- Downloading of all files is allowed.

Using This User's Guide

This User's Guide is designed to install, configure, use, and troubleshoot the NetPurifier network content filtering device. The following list summarizes the chapters and appendixes that follow this chapter.

- Chapter 2, "Installing NetPurifier"— describes how to install and physically connect NetPurifier to your network.
- Chapter 3, "Configuring NetPurifier"— describes how to configure NetPurifier. This includes setting up DHCP, DNS, Gateway and changing Sensitivity Levels
- Chapter 4, "NetPurifier Operation"— describes the operation of NetPurifier.
- Appendix A, "Troubleshooting" — provides information for troubleshooting NetPurifier.
- Appendix B, "Contact Information" —provides contact information including telephone numbers, address, email and hours of operation.
- Appendix C, "Specifications" — provides technical information about NetPurifier.

For your convenience, an Index appears at the end of this User's Guide.

Navigating Through This Online User's Guide

This User's Guide contains all the information you need to install, use, and troubleshoot NetPurifier. To assist you in navigating

through this document, we have added blue-colored hot links to the Table of Contents, index, chapters, and appendixes in this User's Guide. Clicking one of these hot links automatically moves you to that location in this User's Guide. For example, if you click one of the blue-colored chapter or appendix titles in the previous section, you automatically move to the first page in that chapter or appendix.

Conventions in This User's Guide

This User's Guide uses the following conventions:

- "Notes" are information requiring extra attention.
- "Tips" are helpful procedures or shortcuts for simplifying a task.
- "Important" is information that, if not followed, may affect the proper operation of the product.
- "Warning" is information, that if not followed or understood, may affect the operation of the product, the operating system or the system configuration.
- "**Bold**" is used to denote an item that is to be clicked or selected.

Getting Started

NetPurifier suggests that the following order of installation and configuration is followed.

1. Have the following information available when installing and configuring NetPurifier.

   Network IP range _____

   (i.e. 192.168.1.0-254)

   Network subnet mask _____

   (i.e. 255.255.255.0)

   Primary DNS _____

   Secondary DNS _____

   Network Gateway _____

If you will be using Net Purifiers built-in DHCP server the following additional information may be needed.

Static IP device 1 _____

Static IP device 2 _____

Static IP device 3 _____

2. Install NetPurifier as described in Chapter 2, Installing NetPurifier.
3. Configure NetPurifier as described in Chapter 3, Configuring NetPurifier.

Chapter 2

Installing NetPurifier

In this chapter we will discuss the physical installation of NetPurifier and how to connect a browser to NetPurifier in preparation for configuration.

Installation

Location

NetPurifier should be installed in a clean, dry location located within near available hub/switch port of the network that is to be filtered.

AC Power

Connect the supplied AC Power cord to the NetPurifier and a properly grounded 115VAC outlet.

Network Connection

Connect either the supplied network cable (6ft) or your own network cable between the NetPurifier's network connector and a port on your hub or switch. NetPurifier works on 10baseT and 100baseT networks.

Note:	NetPurifier may be connected to any point in the network as long as it is on the same subnet as the network it will filter.

Power On and Indicator Lights

After all connections are made NetPurifier may be powered on by pressing the power switch on the front of the unit. The green indicator light indicates that NetPurifier is powered on and functioning normally. The yellow light indicates disk activity.

Note:	After power on, NetPurifier will take approximately two minutes before it is ready for operation.

To power off NetPurifier press the power button. All indicator lights will extinguish.

Connecting a browser to NetPurifier

Configuration of NetPurifier is done by way of TCP/IP using a Browser. The following browsers have been tested with NetPurifier.

Internet Explorer 4 or newer
Netscape 4 or newer
Opera

NetPurifier is configured from the factory for the 192.168.1.0/255.255.255.0 subnet. If your network is already using this subnet then you are ready to configure NetPurifier.

If your network is not using this subnet then you will need to configure the computer that will configure NetPurifier to temporarily reflect a static IP on the 192.168.1.x network. This is done as follows:

Windows 2000/XP

1. Right click My Network Places
2. Click Properties of the Local Area Network you are using.
3. Double click Internet Protocol.
4. Set the IP address, Subnet mask and Default gateway as shown in Fig 2-1.

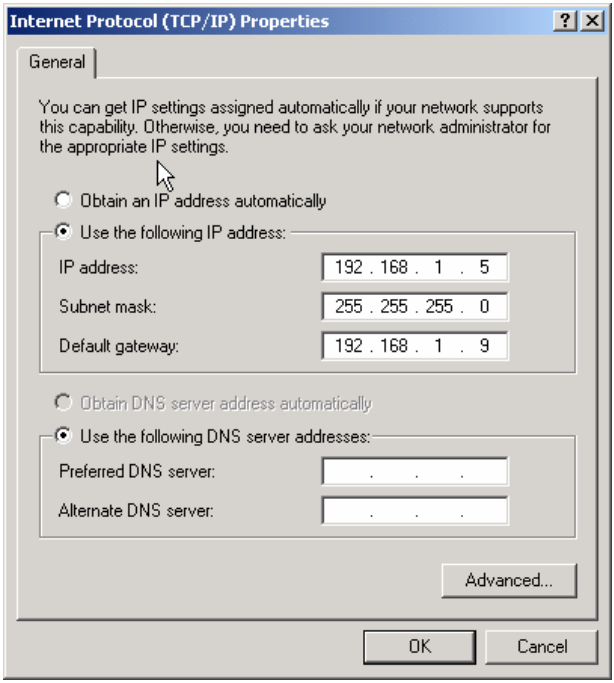
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 5
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168 . 1 . 9
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 2-1: Setting Windows2000/XP IP Address

MAC OS10

Note:	After configuring NetPurifier to your network subnet you may then set your computer back to its original network settings.

Making a connection

NetPurifier is accessed by pointing your browser to 192.168.1.9:10000. Upon a successful connection you will see:

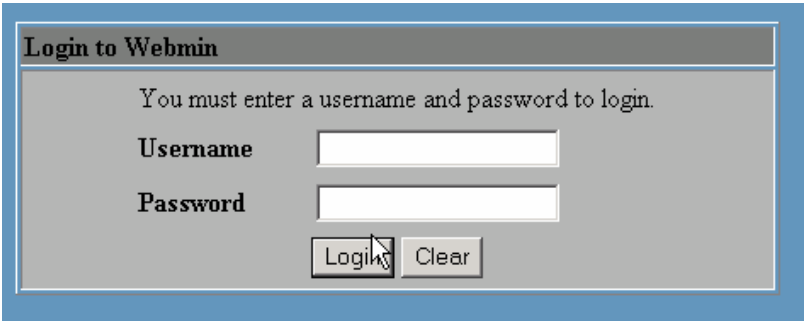

Figure 2-2: Webmin Login

You are now ready to configure NetPurifier as described in the next chapter.

Chapter 3

Configuring NetPurifier

Security Configuration

Upon connection to NetPurifier you will be presented with a login screen to Webmin. Webmin is the web based interface used to configure NetPurifier.

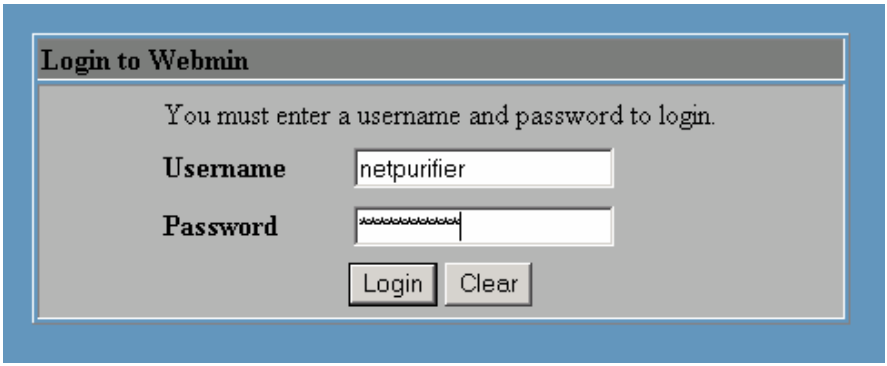

Figure 3-1: Webmin Login

The default Username is: netpurifier
The default Password is: netpurifier

Note:	It is recommended that you immediately change the default password to a password of your own choosing. This is described below.

Changing the default password

Upon successful login you will be presented with the Webmin interface.

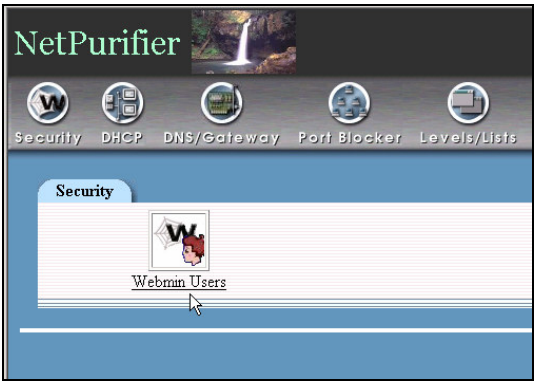

Figure 3-2: Select Webmin Users

After clicking on **Security** you will be presented with a choice of Webmin Users. Clicking on **Webmin Users** will bring up the Webmin Users menu.

By clicking on **netpurifier** you will be able to change the default password.

Changing Default Password

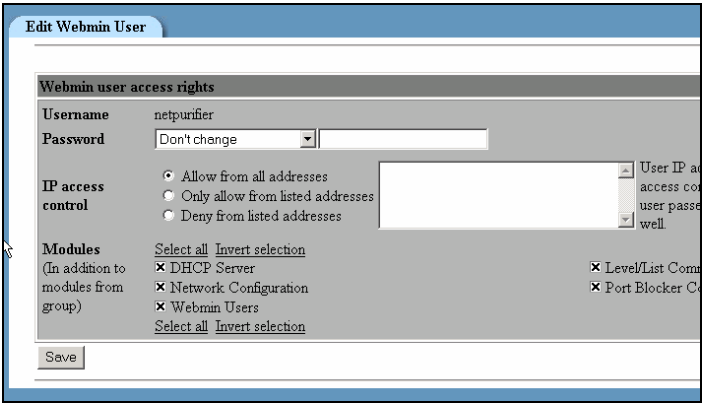

Figure 3-3: Changing Default Password

To change the default password enter the new password, change the Password drop down selection to **set to**, click on **Save.**

Important:	NetPurifier is factory configured to allow login access from any computer on the local network (after proper authentication). This access may be further limited by entering the IP of only the computer(s) that you want configuring NetPurifier in the User IP Access control dialog box.

DNS/Gateway Configuration

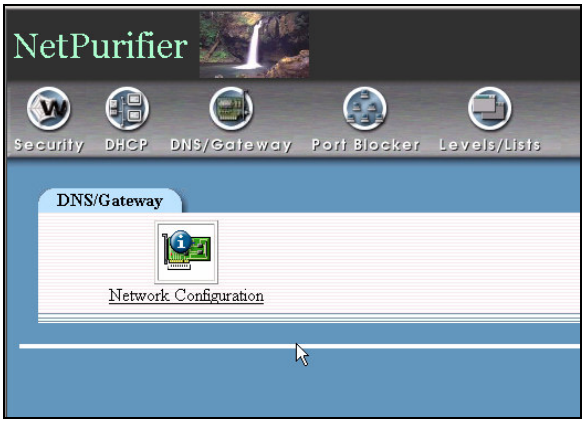

Figure 3-4: Select Network Configuration

In this section the DNS and Gateway settings of your network will be configured.

To access these settings click on **DNS/Gateway** and then on **Network Configuration**. You will be presented with the following choices:

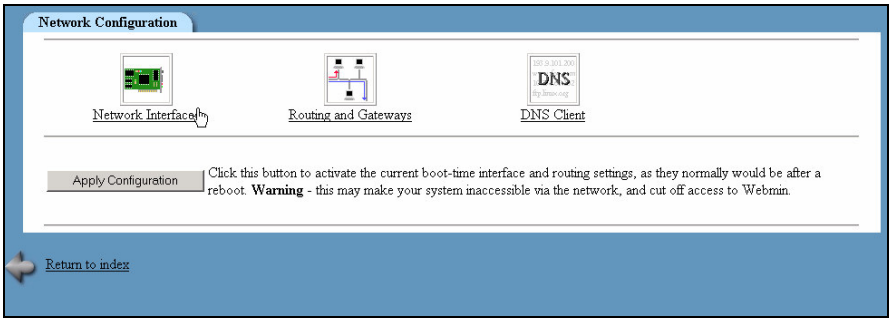
Network Configuration
Network Interfaces
Routing and Gateways
DNS
DNS Client
Apply Configuration
Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. Warning - this may make your system inaccessible via the network, and cut off access to Webmin.
Return to index

Figure 3-5: Network Configuration Choices

Network Interfaces (IP Address Configuration)

NetPurifier is factory configured to an IP of 192.168.1.9 with a subnet mask of 255.255.255.0. If your network does not use this subnet then change the IP of NetPurifier as described in this section.

Click on **Network Interfaces**. This will expose the Active Interfaces Now dialog.

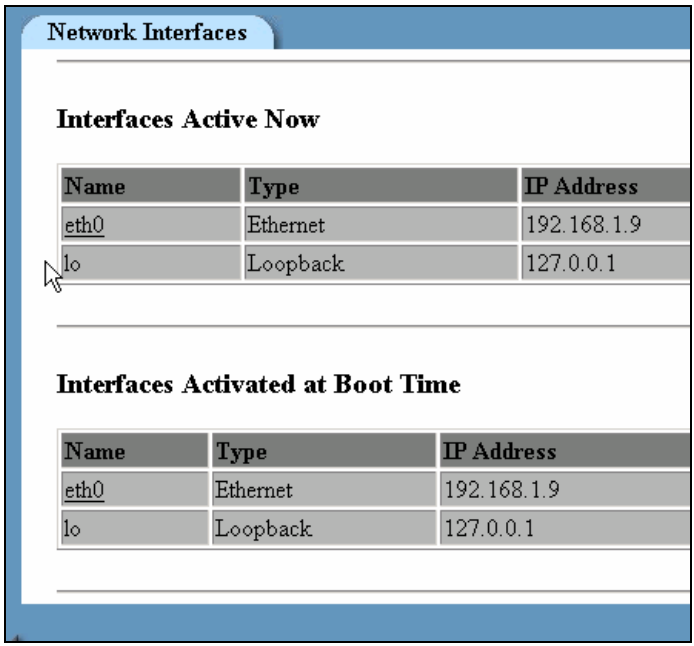

Figure 3-6: Selecting Network Interface

Click on **Interfaces Activated at Boot Time**. This will expose the Active Interface Parameters

Warning:	Entering the wrong IP address and subnet mask will cause you to lose communication with NetPurifier. If you do not remember the information entered you will not be able to reconnect with NetPurifier.

Change the Netmask and IP Address to reflect your network requirements.

When completed click on **Save.**

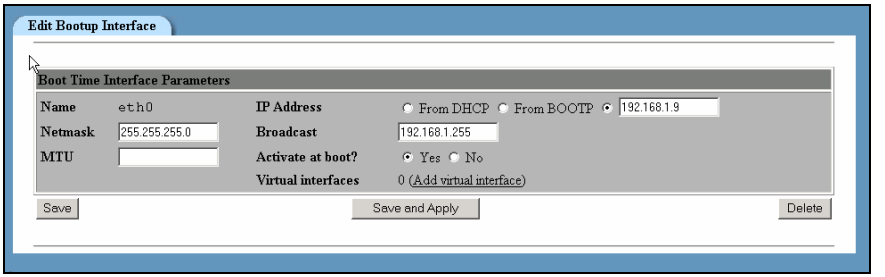

Figure 3-7: Entering IP and Subnet Mask

Continue to the next section, Routing and Gateways.

Routing and Gateways

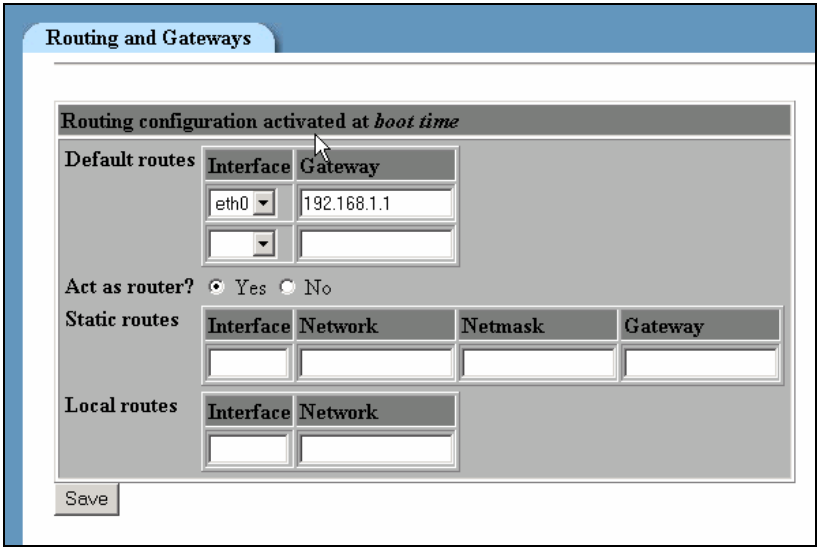

Figure 3-8: Entering Gateway IP

Enter the IP address of the Internet Gateway that NetPurifier will use to access the Internet. This may be the same Internet gateway address as client computers were previously using to access the Internet.

When completed click on **Save.**

Continue to the next section, DNS.

DNS

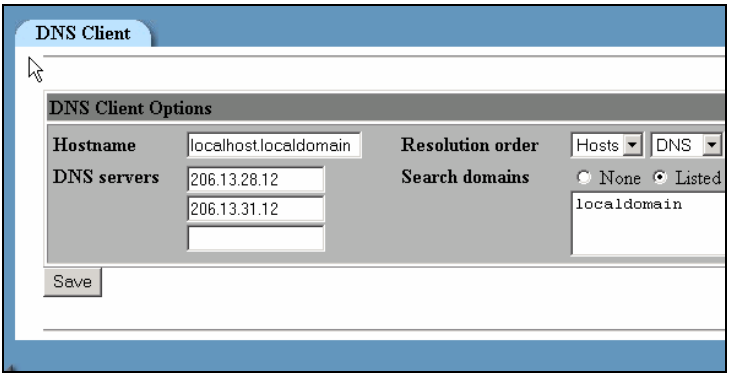

Figure 3-9: Entering DNS Settings

Enter the DNS settings that NetPurifier will use to resolve Domain Names. These may be the same DNS servers that the client computers are using.

When completed click on **Save**.

Completing the DNS/Gateway Configuration

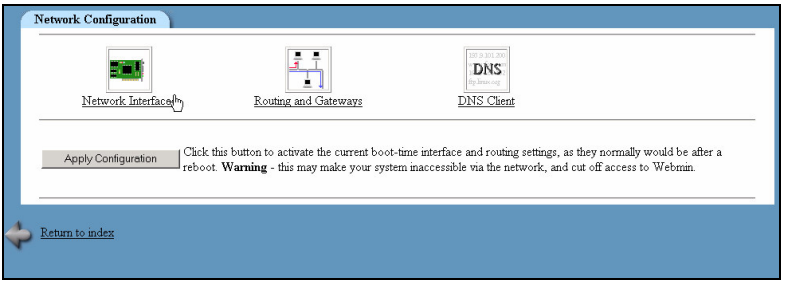
Network Configuration
Network Interfaces
Routing and Gateways
DNS
DNS Client
Apply Configuration
Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. Warning - this may make your system inaccessible via the network, and cut off access to Webmin.
Return to index

Figure 3-10: Apply Configuration

The final step in completing the DNS/Gateway configuration is to click the **Apply Configuration** button

Warning:	This step will change the IP of NetPurifier. You must reconfigure the computer you are using to configure NetPurifier to reflect the new IP and subnet.

DHCP Configuration

NetPurifier can operate in conjunction with an existing DHCP server or with its own built-in DHCP server. In either case the key to the successful operation of NetPurifier is a redirect of the Internet Gateway IP address from the true Internet Gateway to NetPurifier. This allows NetPurifier to sit between the requesting computer and the true Internet Gateway.

Using an existing DHCP Server

If using an existing DHCP Server the following items must be configured:

1. Set Net Purifiers DNS/Gateway setting to reflect your networks IP Subnet.
2. Change your existing DHCP server to point client computers to the NetPurifier IP (gateway)

Using the NetPurifier DHCP Server

NetPurifier has a built in DHCP server. It is factory configured but not activated when shipped. If you use the NetPurifier DHCP server you will need to modify the existing factory configuration to meet your network parameters, save the configuration and Start the DHCP server

Factory Configuration

Following are the factory settings for the DHCP server:

- Scope 192.168.1.10 – 192.168.1.240
- Subnet Mask 255.255.255.0
- Default Router 192.168.1.9
- Default Gateway 192.168.1.1
- Broadcast Address 192.168.1.255
- Lease Time 7 days

Setting up the Subnet

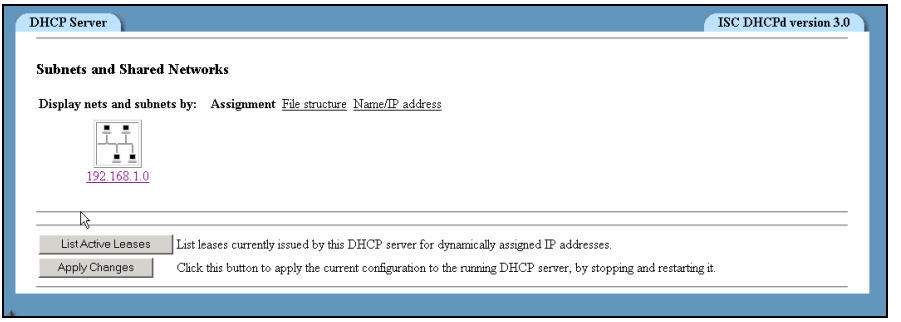
DHCP Server
ISC DHCPd version 3.0
Subnets and Shared Networks
Display nets and subnets by: Assignment File structure Name/IP address
192.168.1.0
List Active Leases
List leases currently issued by this DHCP server for dynamically assigned IP addresses.
Apply Changes
Click this button to apply the current configuration to the running DHCP server, by stopping and restarting it.

Figure 3-11: Selecting Network

Click on the current IP address as shown above to expose the DHCP subnet settings

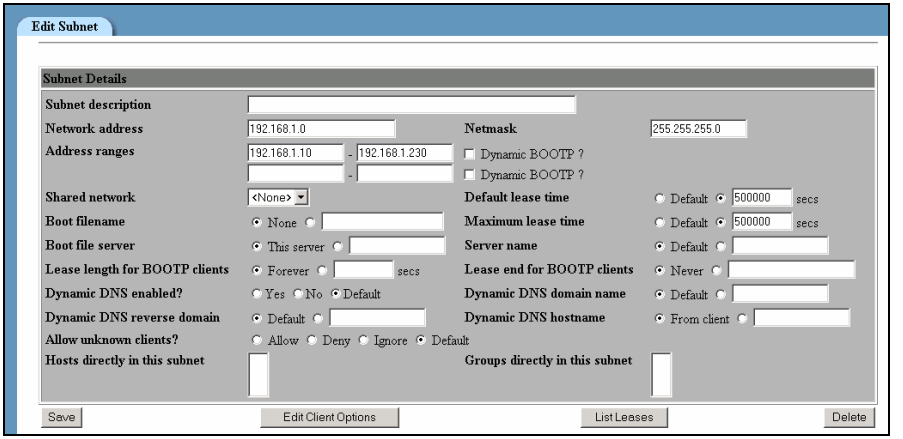

Figure 3-12: Setting the DHCP Subnet

The above example shows the factory defaults for setting the DHCP Subnet. If your network uses a different subnet then replace the values shown with your network's settings.

Edit Client Options

The example below shows the factory defaults for setting the DHCP Client options If your network uses different settings then replace the values shown with your network's settings.

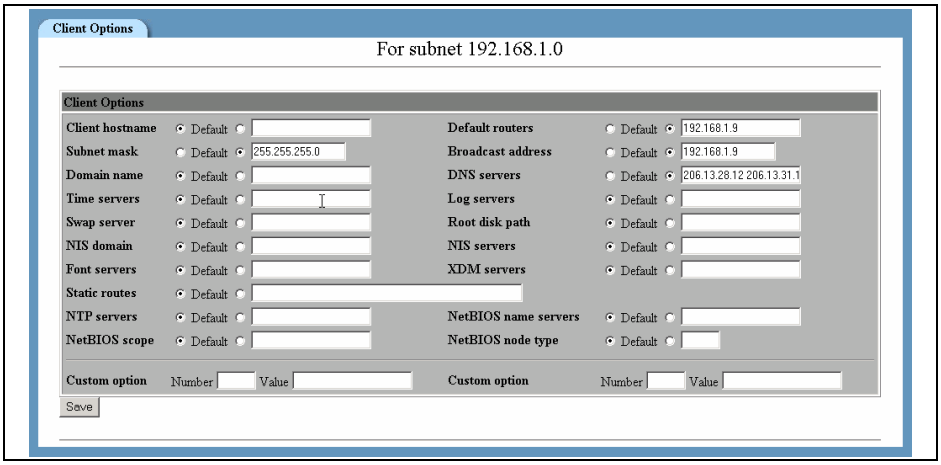

Figure 3-13: Entering Client DHCP Option

Starting and Stopping the DHCP Server

Upon completion of configuring the DHCP server the server must be started. Click on **Apply Changes** - **Start Server,** as shown in Fig. 3-13, to accomplish this task.

Port Blocker

Port Blocker allows the selective enabling and disabling of ports. This can restrict or allow the use of certain applications such as email, peer-to-peer music sharing and instant messenger chat. By default Port Blocker allows all ports.

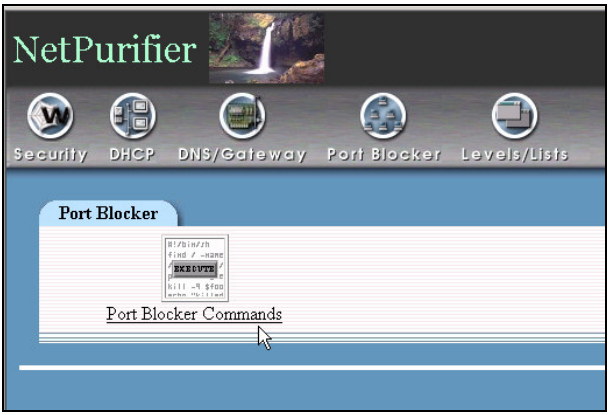

Figure 3-14: Port Blocker Commands

Note:	Port Blocker *is not a firewall*. NetPurifier is designed to sit inside the trusted network. It will block ports to and from the firewall to control application access but is not designed to protect the network from outside factors.

Changing Port Blocker Configuration

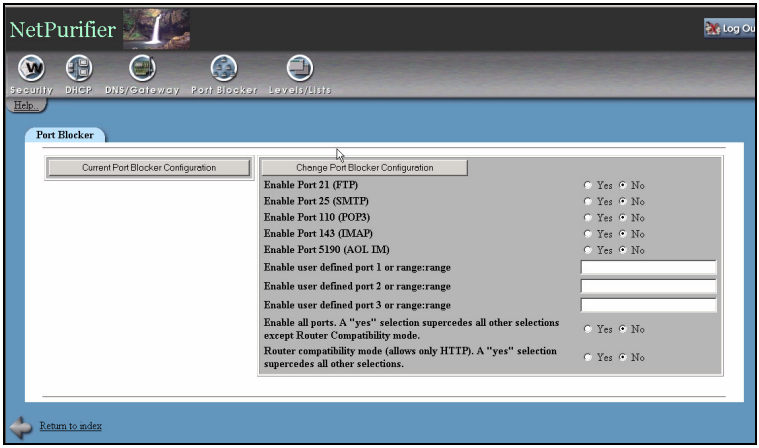
NetPurifier
Log Ou
Security
DHCP
DNS/Gateway
Port Blocker
Levels/Lists
Help
Port Blocker
Current Port Blocker Configuration
Change Port Blocker Configuration
Enable Port 21 (FTP)
Enable Port 25 (SMTP)
Enable Port 110 (POP3)
Enable Port 143 (IMAP)
Enable Port 5190 (AOL IM)
Yes No
Enable user defined port 1 or range:range
Enable user defined port 2 or range:range
Enable user defined port 3 or range:range
Enable all ports. A "yes" selection supercedes all other selections except Router Compatibility mode.
Router compatibility mode (allows only HTTP). A "yes" selection supercedes all other selections.
Return to index

Figure 3-15: Changing Port Blocker Configuration

Enabling Common Ports

To enable services such as FTP, email and instant messenger click on the **Yes** button for the service and then click **Change Port Blocker Configuration**. When **Change Port Blocker Configuration** is clicked NetPurifier will close all ports and then open only the ports that have been selected.

Note:	Port Blocker will never block browser access to the Internet (Port 80). Additionally certain ports are required to be open to allow proper operation of various applications.

Note:	Port Blocker does not affect access to web based email such as Hotmail or Yahoo Mail. Control of web based email is accomplished through Sensitivity Levels. Port Blocker does affect the operation of client based email such as Outlook, Outlook Express and Eudora.

Adding User Defined Ports

If a port is not listed it may be entered manually by entering the port number in User Defined Ports. A range of ports may be entered by using range:range.

Enabling All Ports

Enabling all ports opens all ports. This is the default setting of NetPurifier.

Router Compatibility Mode

NetPurifier uses latest generation Statefull Packet Inspection (SPI) to determine ports that should be opened or closed in response to settings in Common Ports. This allows programs that are wanted to be let through and programs that are not wanted to be blocked. Older generation routers are not aware of this technology and may not operate properly with Port Blocker. If certain applications (such as email or FTP) do not work as expected after configuring port blocker then there may be a router compatibility issue.

If such an issue is determined there are two courses of action that may be followed.

- Enable Router Compatibility mode. This mode allows only Port 80 to be open. Web access is allowed. All other ports are blocked.
- Enable all Ports. This will open all ports and allow all applications to connect.

Changing levels, lists and messages

Changing Levels

Changing Sensitivity Levels on NetPurifier is as simple as clicking on the level desired. When clicked the level is changed and NetPurifier is restarted. Each level and its filtering capabilities are described below in the Filter Matrix.

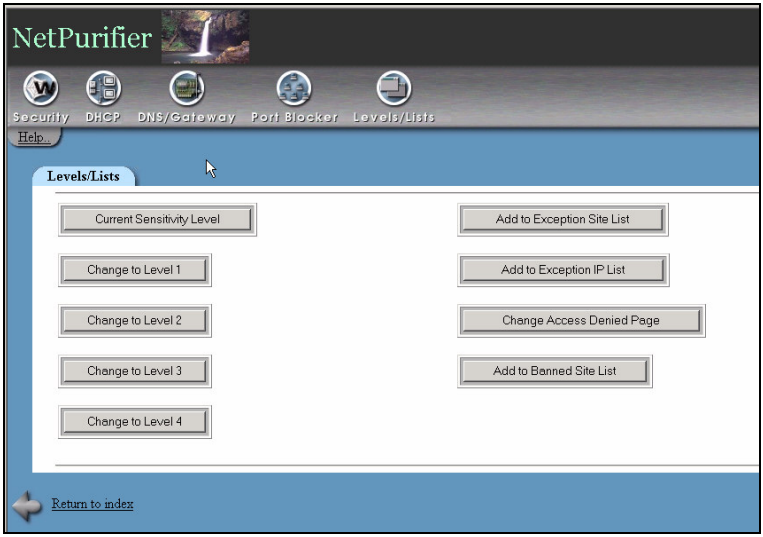

Figure 3-16 Changing Sensitivity Levels

Note:	Upon changing a level NetPurifier will restart with the new level. A restart may take up to one minute to complete. During this time user access to the Internet will be denied.

Filter Matrix

Smart Filter Technology

B=banned	Description	Level 1	Level 2	Level 3	Level 4
Smart Filter Threshold		50	100	150	200

Banned Sites Filter

B=banned	Description	Level 1	Level 2	Level 3	Level 4
Banned Sites					
ads		B	B	B	
aggressive		B	B	B	
audio-video		B	B	B	
drugs		B	B	B	
gambling		B	B	B	
hacking		B	B	B	
mail		B	B		
porn		B	B	B	B
proxy		B	B	B	
violence		B	B	B	
warez		B	B	B	

PICS Filter

B=banned	Description	Level 1	Level 2	Level 3	Level 4
PICS Ratings		On	On	On	Off

Banned File Extensions

B=banned	Description	Level 1	Level 2	Level 3	Level 4
.cpl	Control Panel extension	B			
.crt	Security certificate	B			
.dll	Windows system file	B			
.exe	Program	B	B	B	
.hlp	Help file	B			
.ini	Windows system file	B			
.hta	HTML program	B			
.inf	Setup Information	B			
.ins	Internet Naming Service	B			
.isp	Internet Communication settings	B			
.lnk	Windows Shortcut	B			
.mda	Microsoft Access add-in program	B			
.mdb	Microsoft Access program	B			
.mde	Microsoft Access MDE database	B			
.mdt	Microsoft Access workgroup information	B			
.mdw	Microsoft Access workgroup information	B			
.mdz	Microsoft Access wizard program	B			
.mdz	Microsoft Access wizard program	B			
.msc	Microsoft Common Console document	B			
.msi	Microsoft Windows Installer package	B			
.msp	Microsoft Windows Installer patch	B			
.mst	Microsoft Visual Test source files	B			
.pcd	Photo CD image, Microsoft Visual compiled script	B			

B=banned	Description	Level 1	Level 2	Level 3	Level 4
.pif	Shortcut to MS-DOS program	B			
.prf	Microsoft Outlook profile settings	B			
.reg	Windows registry entries	B			
.scf	Windows Explorer command	B			
.scr	Screen saver	B			
.sct	Windows Script Component	B			
.sh	Shell script	B			
.shs	Shell Scrap object	B			
.sys	Windows system file	B			
.url	Internet shortcut	B			
.vb	Internet shortcut	B			
.vbe	VBScript Encoded script file	B			
.vbs	VBScript file	B			
.vxd	Windows system file	B			
.wsc	Windows Script Component	B			
.wsf	Windows Script file	B			
.wsh	Windows Script Host Settings file	B			
.otf	Font file - can be used to instant reboot 2k and xp	B			
.ops	Office XP settings	B			
.doc	Word document	B			
.xls	Excel document	B			
.gz	Gziped file	B			
.tar	Tape ARchive file	B			
.zip	Windows compressed file	B			
.tgz	Unix compressed file	B			
.bz2	Unix compressed file	B			

B=banned	Description	Level 1	Level 2	Level 3	Level 4
.cdr	Mac disk image	B			
.dmg	Mac disk image	B			
.smi	Mac self mounting disk image	B			
.sit	Mac compressed file	B			
.sea	Mac compressed file, self extracting	B			
.bin	Mac binary compressed file	B			
.hqx	Mac binhex encoded file	B			
.rar	Similar to zip	B			
.mp3	Music file	B	B	B	
.mpeg	Movie file	B			
.avi	Movie file	B			
asf	this can also exploit a security hole allowing virus infection	B			
.iso	CD ISO image	B			
.ogg	Music file	B			
.wmf	Movie file	B			
.bin	ISO image	B			
.cue	CD ISO image	B			

Adding to the Exception Site list

To access the Exception Site list click on **Exception Site List.**

Place sites that you wish to except from NetPurifier filtering in the Exception Site List.

Figure 3-17: Adding to the Exception Site List

Note:	When entering sites in the list you do not need to preface with www. A # sign will cause the entry to be ignored.

When completed click on **Save**.

Adding to the Exception IP list

To access the Exception IP list click on **Exception IP List**.

Place the IP's of computers that you do not want filtered by NetPurifier in this list. This may include administrator workstations and servers.

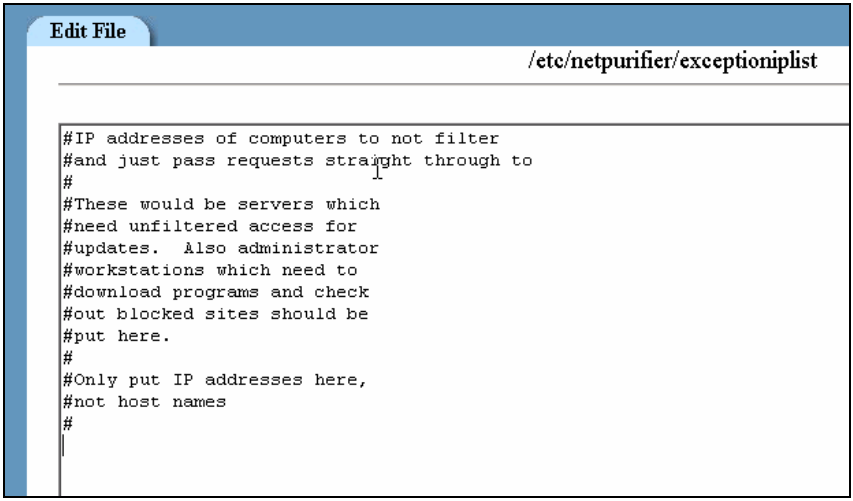

Figure 3-18: Adding to the Exception IP List

Note:	When entering sites in the list use the standard IP (i.e. 192.168.1.1). A # sign will cause the entry to be ignored.

When completed click on **Save**.

Changing the Access Denied page message

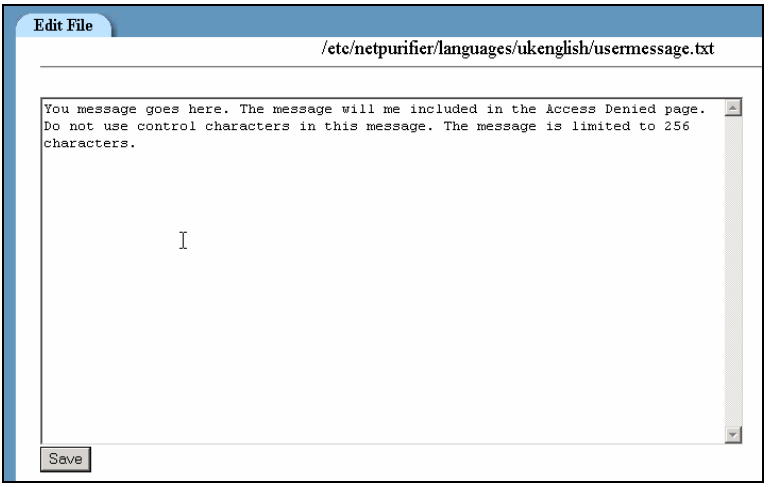
Edit File
/etc/netpurifier/languages/ukenglish/usermessage.txt
You message goes here. The message will me included in the Access Denied page.
Do not use control characters in this message. The message is limited to 256
characters.
Save

Figure 3-19: Changing Access Denied Message

When NetPurifier determines that an Internet page should not be shown to the requesting user an “Access Denied” page is sent to the user. The page shows what site was not allowed, the reason why and a message that may be configured to meet your requirements.

Enter the message that you would like to appear on the “Access Denied” page.

When completed click on **Save**.

Note:	Upon changing the Access Denied message NetPurifier will restart with the new message available. A restart may take up to one minute to complete. During this time user access to the Internet will be denied.

Add to Banned Site List

If a site is found that you believe should be banned it may be easily added using the Banned Site List.

To add a site, enter the name of the site. It is not necessary to use the www prefix.

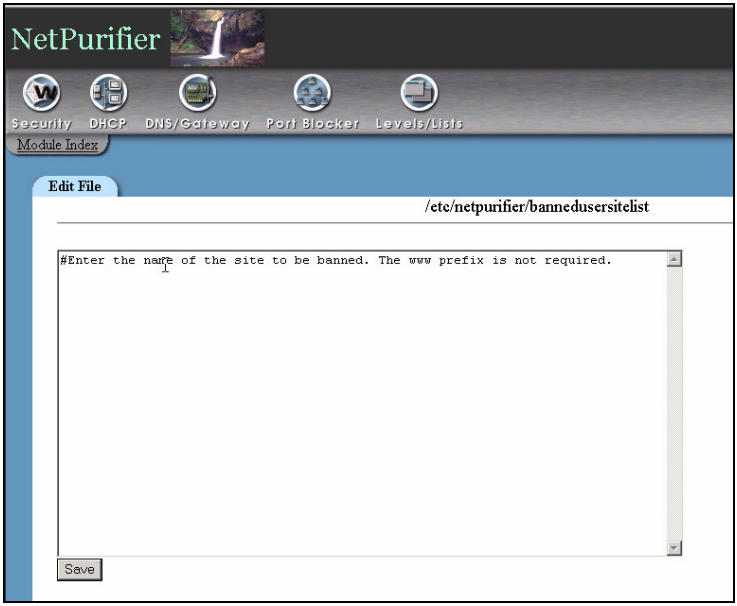

Figure 3-20: Banned Site List

When completed click on **Save**.

Note:	Upon changing the Banned Site List, NetPurifier will restart. A restart may take up to one minute to complete. During this time user access to the Internet will be denied.

Chapter 4

NetPurifier Operation

NetPurifier operates as an in-line filter between the requesting computer and the Internet. The diagram below shows how a request is routed through NetPurifier

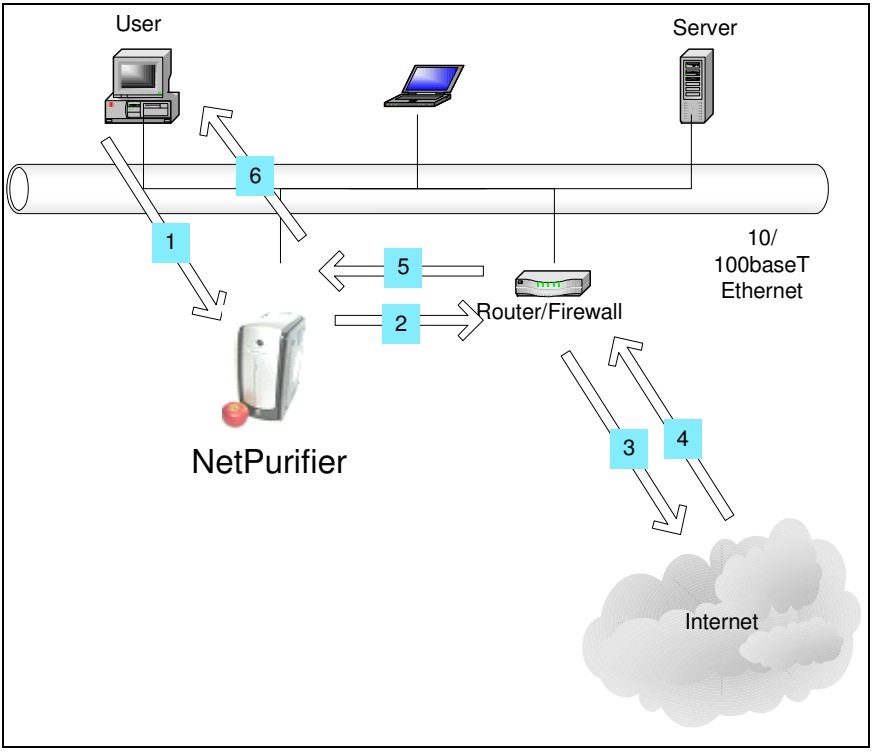

Figure 4-1: NetPurifier Operation

Network Flow

1. User requests web page (1). NetPurifier checks internal cache for page. If locally cached, NetPurifier responds to request immediately (6).
2. If not locally cached NetPurifier requests page from Internet by way of Router/Firewall (2).
3. Request for page is sent to Internet (3).
4. Request is received from Internet (4).
5. Returned page is routed to NetPurifier (5).
6. If clean NetPurifier serves page to end user (6). If not clean NetPurifier sends "Access Denied" page (6).

How NetPurifier filters

Three levels of filtering insure that NetPurifier will stop inappropriate content.

1. NetPurifier first checks the requested URL against its Exception IP List to see if the site is excepted.
2. Next NetPurifier checks the URL against it Exception Site list to see if it is excepted.
3. Next NetPurifier checks the URL against its blacklist. This list has over 500,000 entries and is categorized by content.
4. NetPurifier then loads the complete page into memory and scans it for its PIC's rating. The PIC's rating is then compared with the PIC's list.
5. NetPurifier then scans every word on the page and applies its Smart Filter Technology to determine if the page is acceptable or not.
6. If acceptable the page is sent to the requesting computer.
7. If the page is deemed unacceptable the "Access Denied" page is sent to the requesting computer.

Blacklist

NetPurifier maintains a Blacklist of sites that have been deemed unacceptable. The list is categorized as follows:

Categories

Advertising
Aggressive
Audio-video
Drugs
Gambling
Hacking
Mail
Pornography
Proxy
Violence
Warez

Blacklist Update

The staff at NetPurifier constantly adds and removes sites from its blacklists. NetPurifier will update its blacklists either daily or weekly, depending on the service contract you have acquired.

- The daily update is performed between 2:00 and 4:00 AM local time.
- The weekly update is performed Sunday mornings between 2:00 and 4:00 AM local time.
- The update is automatic and requires no user intervention.

Note:	Upon a Blacklist update NetPurifier will restart with the new list. A restart may take up to one minute to complete. During this time user access to the Internet will be denied.

Smart Filter Technology

Blacklists and the PICs rating system are very effective if the offending web site is known and if they properly rate themselves. 100's of new sites catering to pornography and other inappropriate content are added to the Internet weekly.

To insure that these sites are blocked, until they can be added to the Blacklist, NetPurifier uses Smart Filter Technology. Smart Filter scans and assigns a numeric weight to each word on the requested page. Appropriate words are assigned a negative value while inappropriate words are assigned a positive value. NetPurifier then adds these weights together and derives a value for the page. This value is then compared with the Smart Filter threshold described in Chapter 3. If the threshold is exceeded the page is denied. If the threshold is not exceeded the page is displayed.

An example of this in action is a search engine search for "nude breasts". The page will be denied as it brings up multiple pornographic sites and the threshold is exceeded.

A search on the phrase "breast cancer" is not blocked. The good words found on the page modify the bad words—allowing the page to be displayed.

Note:	Smart Filter is biased to "not show the page if in doubt". This reduces the chance that children will be exposed to inappropriate content. As a result of this bias there may be cases where a user believes they have entered a very safe query but the page is blocked. If so, a more defined search may bring better results. Using the example above a search on "breast cancer" will yield better results than "breast" Even better word be "breast cancer research".

Appendix A

Troubleshooting

Appendix B

Contact Information

For your convenience, NetPurifier provides a number of ways for you to contact us.

Location

NetPurifier, Inc. is located at:

1646 Elderberry Way
San Jose, CA 95125

Phone,	Main	866-875-1254 (toll free in U.S.)
	Sales	866-875-1254 (toll free in U.S.)
	Support	866-875-1254 (toll free in U.S.)
	Fax	408-265-5249

Website

Our website is at http://www.netpurifier.com (If you're reading this document as a PDF file and are currently on-line, please click the URL above and you'll be transported to our website.) On our website, you will find the latest information about our leading-edge solutions, product announcements along with a form you can use for general information requests.

Sales

Our friendly and knowledgeable sales staff is available to answer your sales-related questions. Hours of operation are from Monday through Friday, 8:00am to 5:00pm Pacific Time at 866 875-1254.

Technical Support

NetPurifier provides technical phone support at 866 875-1254. Email support is available at support@netpurifier.com. You can also fax your questions to us at our 24-hour fax number: 408-265-5249.

Appendix C

Specifications

Network

Network Type - 10/100baseT
NetPurifier operates in a Network Address Translation mode (NAT). In this mode only non-routable IP addresses are used on the internal LAN (192.xxx.xxx.xxx).

Number of Computers

When used with it's built in DHCP server, NetPurifier is configured to allow access to up to 230 computers.

Typical Access Time

Access time per HTTP request is less than 20ms.

DHCP Requirements

NetPurifier is configured with an active DHCP server. The scope is 192.168.1.10 to 192.168.1.249. 192.168.1.1 is reserved for the Internet Gateway. 192.168.1.9 is reserved for NetPurifier. 192.168.1.250-253 is reserved for wireless devices that may be present on a network. The DHCP server is easily disabled if an existing DHCP server is used. In this case the existing DHCP server will need to redirect its DHCP client's gateway to NetPurifier.

Port Requirements

Port 80 for standard HTTP operation
Port 10000 for remote configuration

Caching Proxy

NetPurifier incorporates a caching proxy that caches web pages that have been accessed and filtered. Subsequent accesses to these pages are served from the caching proxy – not from the Internet. Access time from the cache is near instantaneous and depending on network usage patterns may result in a substantial reduction in Internet network traffic.

Blacklist Update

The Blacklist is updated automatically between 2:00 and 4:00 AM daily local time or between 2:00 and 4:00 AM Mondays, depending on the Service Contract. The update takes approximately 2 minutes over a typical 1.5mbps line.

Mechanical & Environmental

Dimensions – HxWxD 11.5" x 5.5" x 10.5"
Weight – 10 lbs
Electrical 115VAC, 75watts